

# On quadratic non-residues

March 5, 2007

## 1 Introduction

Vinogradov's conjecture (actually, a special case of the conjecture), a major unsolved problem in number theory, claims the following:

For every  $\varepsilon > 0$  and  $p$  a sufficiently large prime, there exists an integer  $n$  satisfying  $|n| \leq p^\varepsilon$ , such that  $n$  is a quadratic non-residue modulo  $p$ .

From the fact that  $(-1/p) = -1$  for  $p \equiv 3 \pmod{4}$ , to prove this conjecture, one just needs to do so for the case  $p \equiv 1 \pmod{4}$ .

Currently, the best results on this conjecture are due to Burgess [2], who showed that it holds for all  $\varepsilon > 1/4\sqrt{e}$ . Actually, what Burgess showed was that for every integer  $x$ , one has the estimate

$$\left| \sum_{x < n < x + p^{1/4} \log p} (n/p) \right| = o(p^{1/4} \log p).$$

However, applying this estimate with  $x = 0$ , one sees that it is saying that there are asymptotically as many quadratic residues as non-residues up to  $p^{1/4} \log^c p$ ; and, if all those  $1 \leq n < p^{1/4\sqrt{e}+\delta}$  were quadratic residues modulo  $p$ , then since a little more than half of the  $n \leq p^{1/4} \log^c p$  have all their prime factors smaller than  $p^{1/4\sqrt{e}+\delta}$ , we would have that the quadratic residues up to  $p^{1/4} \log^c p$  greatly outnumber the quadratic non-residues. This then would be a contradiction, and so Vinogradov's conjecture holds for all exponents exceeding  $1/4\sqrt{e}$ .

In the present paper we will present a novel method for attacking Vinogradov's conjecture. We will begin by considering the case  $\varepsilon > 1/2$ , where we will show that the method succeeds, although this was a case long known to hold (even before Burgess) and has many nice proofs; see, for example, [1] and [4], and [3] for the treatment of a special case. Then, in a later section, we will state a general theorem (Theorem 1), which encapsulates the method for the general case  $\varepsilon > 0$ , though we have not yet been able to use the method to handle the case  $0 < \varepsilon \leq 1/2$ .

## 2 The method for $\varepsilon > 1/2$

### 2.1 General discussion of the ideas

Our method is based on the following classical property of the Gauss sum: If

$$G(a) = \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) e^{2\pi i a n/p},$$

then

$$G(a) = \left(\frac{a}{p}\right) G(1).$$

Further, we have that if  $p \equiv 1 \pmod{4}$ , then  $G(1) = \sqrt{p}$ , which gives

$$G(a) = \left(\frac{a}{p}\right) \sqrt{p}.$$

If  $(a/p) = +1$  for all  $|a| \leq p^\varepsilon$ ,  $a \neq 0$ , then we observe that, with the exception of the point  $a = 0$ ,  $G(a)$  is the constant function  $\sqrt{p}$ . It turns out that we can use this fact to produce a good rational approximation to the number  $\sqrt{p}$ , and we will show that this approximation must be too good to be true, at least when  $\varepsilon > 1/2$ .

The way that we build our rational approximations is that we first construct a function

$$f : \mathbb{F}_p \rightarrow \mathbb{Z},$$

which has two nice properties described below, and then assuming that  $(n/p) = +1$  for all non-zero  $|n| < p^\varepsilon$ , we will use this function to form

the rational approximation

$$\sqrt{p} \approx \frac{p\hat{f}(0) - pf(0)}{pf(0) - \hat{f}(0)}.$$

Roughly, the way we will derive this approximation is to find two expressions for

$$\sum_{|n| < p/2} f(n)(n/p).$$

On the one hand, we will just be able to directly find an expression for it if  $(n/p) = +1$  for all non-zero  $n$  satisfying  $|n| < p^\varepsilon$ ; and, on the other hand, we will be able to find another expression using Fourier transforms and Gauss sums. Equating these two expressions will give us our rational approximation, up to some error. Finally, we will show that the error in this approximation is too good to be true, since quadratic irrationals cannot be too well approximated by rational numbers; and so, we will conclude that  $(n/p) = -1$  for some  $|n| < p^\varepsilon$ .

The two “nice properties” that our function  $f$  should have, in order to make this approach work are, firstly, a “divisibility property”, which just says that  $\hat{f}(0)/f(0) = \alpha/\beta$ , where  $\alpha$  and  $\beta$  are “small” integers; and, secondly, it must have a certain “decay property”, which is just that

$$\sum_{p^\varepsilon < |a| < p/2} |\hat{f}(a)| \text{ is “small”}.$$

We will make both of these requirements more precise in the next subsection.

## 2.2 The construction of $f(n)$

We will build our function  $f(n)$  using linear combinations of certain other functions  $f_N(n)$ , which are perhaps best defined via their Fourier transforms as follows: For an integer  $k \geq 1$  to be determined later (it will depend only on  $\varepsilon$ ), let

$$\hat{f}_N(a) = \left( \sum_{\substack{|n| \leq N \\ n \neq 0}} \omega^{an} \right)^{2k}, \text{ where } \omega = e^{2\pi i/p}. \quad (1)$$

To find  $f_N(n)$  we use Fourier inversion as follows

$$f_N(n) = \frac{1}{p} \sum_{a=0}^{p-1} \omega^{-an} \hat{f}_N(a). \quad (2)$$

On expanding out (1), one can check that

- $f_N(0)$  is a polynomial in  $N$  of degree  $2k - 1$ ; and,
- $\hat{f}_N(0) = (2N)^{2k}$ , which is a polynomial in  $N$  of degree  $2k$ .

By these two statements we mean that for a fixed value of  $k \geq 1$ , there exist polynomials

$$g_1(x), g_2(x) \in \mathbb{Z}[x], \deg(g_1) = 2k - 1, \text{ and } \deg(g_2) = 2k,$$

such that

$$f_N(0) = g_1(N), \text{ and } \hat{f}_N(0) = g_2(N), \text{ for all } N > 0.$$

In fact,  $g_2(x) = (2x)^{2k}$ .

One can clearly find rational numbers  $a_1, \dots, a_{2k}$  such that

$$a_1 g_1(x) + a_2 g_1(2x) + \dots + a_{2k} g_1(2kx) = x^{2k-1}.$$

Then, since  $g_2(x) = (2x)^{2k}$ , we must have that

$$a_1 g_2(x) + a_2 g_2(2x) + \dots + a_{2k} g_2(2kx) = x^{2k} (a_1 2^{2k} + a_2 4^{2k} + \dots + a_{2k} (4k)^{2k}).$$

Further, we can choose these  $a_i$  so that this last linear combination involving  $a_j (2j)^{2k}$  does not vanish. Given such a set of rationals  $a_1, \dots, a_{2k}$ , let

$$f(n) = a_1 f_N(n) + a_2 f_{2N}(n) + \dots + a_{2k} f_{2kN}(n).$$

### 2.2.1 The “divisibility property” for $f(n)$

We first observe that

$$f(0) = a_1 g_1(N) + \dots + a_{2k} g_1(2kN) = N^{2k-1}; \quad (3)$$

and

$$\hat{f}(0) = a_1 g_2(N) + \cdots + a_{2k} g_2(2kN) = N^{2k} \sum_{j=1}^{2k} a_j (2j)^{2k}. \quad (4)$$

Thus,

$$\frac{\hat{f}(0)}{f(0)} = \frac{\sum_{j=1}^{2k} a_j g_2(jN)}{\sum_{j=1}^{2k} a_j g_1(jN)} = N \sum_{j=1}^{2k} a_j (2j)^{2k} = \frac{Nu}{v}, \quad (5)$$

where  $u$  and  $v$  are just certain integers that depend only on  $k$ . This is our “divisibility property” for  $f(n)$ .

### 2.2.2 The “decay property” for $f(n)$

Since  $\hat{f}_N(a)$  is the  $2k$ th power of the sum of two geometric series with common ratio  $\omega^a$ , and since  $f(n)$  is a linear combination of certain  $f_{jN}(n)$ , we deduce from the geometric series formula that

$$|\hat{f}(a)| \ll_k |1 - \omega^a|^{-2k} \ll_k |\sin(\pi a/p)|^{-2k} \ll_k p^{2k}/a^{2k};$$

and so,

$$\sum_{p^\varepsilon < |a| < p/2} |\hat{f}(a)| \ll_k p^{2k} \sum_{a > p^\varepsilon} \frac{1}{a^{2k}} \ll_k p^{2k(1-\varepsilon)+\varepsilon}. \quad (6)$$

## 2.3 Construction of the rational approximation to $\sqrt{p}$

Let us now assume that  $\varepsilon > 1/2$ ; and, for proof by contradiction, assume that the following holds.

**Assumption.**  $(a/p) = +1$  for all non-zero  $a$  satisfying  $|a| \leq p^\varepsilon$ .

In what follows we will use the value

$$N = \lfloor \sqrt{p} \rfloor,$$

which is a parameter that appears in our construction of  $f(n)$ .

Notice that since our function  $f(n)$  appearing in the previous section is a linear combination of functions  $f_{jN}(n)$ ,  $1 \leq j \leq 2k$ , each of which is

supported only on the residues classes mod  $p$  in the interval  $[-4jkN, 4jkN]$ , we deduce that

$$f(n) = 0, \text{ for } 4k^2N < |n| < p/2. \quad (7)$$

Now consider

$$S := \sum_{|n| < p/2} f(n) \binom{n}{p}.$$

Since (7) holds for  $p$  sufficiently large, we deduce that

$$S = \sum_{|n| \leq 4k^2N} f(n) \binom{n}{p}. \quad (8)$$

From our **assumption** above we have that for sufficiently large  $p$ ,

$$S = \sum_{\substack{|n| \leq 4k^2N \\ n \neq 0}} f(n) = \hat{f}(0) - f(0). \quad (9)$$

On the other hand,  $S$  can be expressed in terms of  $\hat{f}(a)$  and  $G(a)$  as follows:

$$\begin{aligned} S &= \frac{1}{p} \sum_{|a| < p/2} \hat{f}(a) G(-a) \\ &= \frac{1}{p} \left( \sqrt{p} \sum_{|a| < p/2} \hat{f}(a) - \sqrt{p} \hat{f}(0) \right) + E \\ &= \sqrt{p} \left( f(0) - \frac{\hat{f}(0)}{p} \right) + E, \end{aligned}$$

where the “error”  $E$  satisfies

$$|E| = \frac{1}{p} \sum_{p^\varepsilon < |a| < p/2} |\hat{f}(a)| \cdot |G(a) - \sqrt{p}| \leq \frac{2}{\sqrt{p}} \sum_{p^\varepsilon < |a| < p/2} |\hat{f}(a)|. \quad (10)$$

Applying our bound (6), we deduce that

$$|E| \ll_k p^{2k(1-\varepsilon)+\varepsilon-1/2}.$$

Equating our two expressions for  $S$  above, we find that

$$\sqrt{p} = \frac{p\hat{f}(0) - pf(0)}{pf(0) - \hat{f}(0)} + F, \quad (11)$$

where

$$|F| = \frac{p|E|}{pf(0) - \hat{f}(0)} \ll_k p^{2k(1-2\varepsilon)+2\varepsilon-1/2}. \quad (12)$$

Here, we have used (3) and (4), along with the fact that  $N \sim \sqrt{p}$ .

Now we use (5) to refine the approximation (11): Dividing numerator and denominator of (11) by  $f(0)$  we have that

$$\sqrt{p} = \frac{pNu - pv}{pv - Nu} + F = \frac{m}{q} + F. \quad (13)$$

Because  $u, v$  can be bounded purely in terms of  $k$  we have that  $q = O(p)$  (we are letting  $p \rightarrow \infty$ ); however, for  $k$  large enough, our bound (12) on the error  $F$  can be made to be smaller than  $1/pq^2$  for  $p$  sufficiently large, since we have assumed  $\varepsilon > 1/2$ . So, we have that

$$\left| \sqrt{p} - \frac{m}{q} \right| < \frac{1}{pq^2}.$$

This is impossible, because on multiplying through by  $\sqrt{p} + m/q$  we find that

$$\left| p - \frac{m^2}{q^2} \right| < \frac{2 \max(\sqrt{p}, m/q)}{pq^2} < \frac{1}{q^2}.$$

We are forced to conclude that our **assumption** is false for  $p$  sufficiently large; and so, we conclude that there exists an integer  $n$  satisfying  $|n| \leq p^\varepsilon$  and  $(n/p) = -1$ .

### 3 Discussion about intervals smaller than $p^{1/2}$

The approach we used in the previous section does not easily extend to intervals of width smaller than  $p^{1/2}$ , and one of the primary reasons is that we do not have an identity comparable to (9) in this case, as we will now explain.

In order to locate quadratic non-residues in the interval  $[-p^\varepsilon, p^\varepsilon]$ , using the method from the previous section, after some thought, one sees that the right sort of  $f(n)$  of the form (1) we should use applies the value for  $N$  given by

$$N = \lfloor p^{1-\varepsilon+\delta} \rfloor, \text{ for some small } \delta > 0.$$

Basically, this value of  $N$  is just right so as to make the errors  $E$  and  $F$  as in (10), (11) and (12), small. Unfortunately, with such a large value of  $N$  (for  $\varepsilon < 1/2$  it will exceed  $p^\varepsilon$ ) we no longer obtain an easy-to-write-down expression of the form (9). Nonetheless, we can still produce a formula of the type (13), where on the left-hand-side we still have  $\sqrt{p}$ , but on the right-hand-side we have a rational number  $m/q$  and then plus  $o(1)$ , where now  $m$  is somewhat more complex than before. If we had that this  $o(1)$  is somewhat smaller than  $1/q^2$ , then we would have a contradiction, as we know that quadratic irrationals such as  $\sqrt{p}$  cannot be so well approximated by rational numbers.

Actually, for some reasons that we do not want to get into, it turns out to be better to try to find good a rational approximation  $m/q$  to the number  $1/\sqrt{p}$ , instead of  $\sqrt{p}$ .

In the next section we will take all these observations into account, and state and prove a general theorem which would imply Vinogradov's conjecture, if a function  $f(n)$  with certain properties could be found.

### 4 The approach to Vinogradov

Here we will prove the following theorem.

**Theorem 1** *Suppose  $p \equiv 1 \pmod{4}$  is prime, and suppose that  $f : \mathbb{F}_p \rightarrow \mathbb{Z}$  is any integer-valued function. We associate to  $f$  the rational number*

$$\frac{m}{q} = \frac{pf(0) - \sum_{|n| < p/2} f(n)}{p \sum_{|n| < p/2} f(n)(n/p)}, \text{ gcd}(m, q) = 1,$$

which is to be thought of as a rational approximation to  $1/\sqrt{p}$

If the following inequality holds

$$\sum_{p^\varepsilon < |a| < p/2} |\hat{f}(a)| < \frac{\sqrt{p}}{8q^2} \left| \sum_{|n| < p/2} f(n)(n/p) \right|, \quad (14)$$

then there must exist an integer  $n$  satisfying  $|n| < p^\varepsilon$  such that  $(n/p) = -1$ .

#### 4.1 Why are the hypotheses reasonable?

First, it is pretty easy to imagine that we could find a function  $f(n)$  such that

$$pf(0) - \sum_{|n| < p/2} f(n) \quad \text{and} \quad p \sum_{|n| < p/2} f(n)(n/p)$$

have a large common factor. In fact, we could easily imagine picking  $f$  so that their ratio  $m/q$  in lowest terms has a value of  $q < p^2$  or perhaps  $p^3$ .

Next, if  $f(n) \geq 0$ , then we might expect that

$$\left| \sum_{|n| < p/2} f(n)(n/p) \right| \gg \frac{\hat{f}(0)}{\sqrt{p}} = \frac{1}{\sqrt{p}} \sum_{|n| < p/2} f(n),$$

because we expect to get “square-root cancellation” due to the oscillating sign of  $(n/p)$ , but the cancellation is often not so extreme that we lose more than a factor  $1/\sqrt{p}$  from the trivial upper bound of  $\hat{f}(0)$  for the sum of  $f(n)(n/p)$  over  $|n| < p/2$ . If so, then (14) is not all that unusual a requirement, because it would follow from an estimate of the type

$$\sum_{p^\varepsilon < |a| < p/2} |\hat{f}(a)| < \frac{cf(0)}{8q^2}$$

for small enough  $c > 0$ ; and, if  $q < p^2$ , then this would be satisfied if

$$\sum_{p^\varepsilon < |a| < p/2} |\hat{f}(a)| < \frac{cf(0)}{8p^4}. \quad (15)$$

Although the  $p^4$  in the denominator looks problematic here, it really isn't if  $\hat{f}(0)$  is at least some large power of  $p$ ; in fact, the function

$$\hat{g}(a) = \left( \sum_{|n| < p^{1-\varepsilon+\delta}} \omega^{an} \right)^{2k}$$

will satisfy an inequality such as (15) for any fixed  $\varepsilon, \delta \in (0, 1]$ , provided that  $k$  is sufficiently large.

The real problem is thus not whether we can satisfy the requirements that  $q$  is small, and that (14) holds, in isolation, but whether we can get them to hold at the same time. One way to maybe approach this is to use the same idea when we constructed  $f(n)$  in previous sections, namely to start with a selection of functions  $f_1, \dots, f_\ell$  such that

$$\sum_{p^\varepsilon < |a| < p/2} |\hat{f}_i(a)| \text{ is small;} \tag{16}$$

and then find some linear combination

$$f(n) = a_1 f_1(n) + \dots + a_\ell f_\ell(n),$$

such that both

$$pf(0) - \sum_{|n| < p/2} f(n) \quad \text{and} \quad p \sum_{|n| < p/2} f(n)(n/p)$$

are both divisible by some large integer  $M$ , so that this large common factor can be cancelled out when we take the ratio of these two integers to produce our  $m/q$ . Of course if (16) holds, and if  $|a_1| + \dots + |a_\ell|$  is not too large, then we will automatically have that

$$\sum_{p^\varepsilon < |a| < p/2} |\hat{f}(a)| \text{ is small,}$$

meaning that we have a chance to satisfy the requirements of Theorem 1.

The main obstacle to implementing this sort of idea is that of keeping  $f(n)$  from being the zero function; that is, we have to find a way to keep the linear combination  $a_1 f_1 + \dots + a_\ell f_\ell$  from producing 0.

## 4.2 Proof of Theorem 1

As in previous sections, let us begin with the following assumption.

**Assumption.** Suppose that  $(n/p) = +1$  for every non-zero  $n$  satisfying  $|n| \leq p^\varepsilon$ .

From this claim we deduce that

$$\begin{aligned} \sum_{|n| < p/2} f(n)(n/p) &= \frac{1}{p} \sum_{|a| < p/2} \hat{f}(a)G(a) = \frac{\sqrt{p}}{p} \sum_{\substack{|a| \leq p/2 \\ a \neq 0}} \hat{f}(a) + E \\ &= \sqrt{p} \left( f(0) - \frac{\hat{f}(0)}{p} \right) + E, \end{aligned}$$

where

$$|E| = \frac{1}{p} \sum_{p^\varepsilon < |a| < p/2} |\hat{f}(a)| \cdot |\sqrt{p} - G(a)| < \frac{2}{\sqrt{p}} \sum_{p^\varepsilon < |a| < p/2} |\hat{f}(a)|.$$

It follows that

$$\frac{1}{\sqrt{p}} = \frac{pf(0) - \hat{f}(0)}{p \sum_{|n| < p/2} f(n)(n/p)} + F = \frac{m}{q} + F,$$

where

$$|F| = \left| \frac{E}{\sqrt{p} \sum_{|n| < p/2} f(n)(n/p)} \right| < \frac{2 \sum_{p^\varepsilon < |a| < p/2} |\hat{f}(a)|}{\left| p \sum_{|n| < p/2} f(n)(n/p) \right|}.$$

Now, from the second assumption in our Theorem, we deduce that

$$|F| < \frac{1}{4\sqrt{p}q^2}.$$

We claim that this is impossible, because it is saying

$$\left| \frac{1}{\sqrt{p}} - \frac{m}{q} \right| < \frac{1}{4pq^2}. \quad (17)$$

To see that this cannot hold, we multiply both sides by  $1/\sqrt{p} + m/q$ , and deduce

$$\left| \frac{1}{p} - \frac{m^2}{q^2} \right| < \frac{2 \max(1/\sqrt{p}, m/q)}{4\sqrt{p}q^2} < \frac{1}{pq^2},$$

since (17) at the very least implies that  $m/q < 2/\sqrt{p}$ .

We have now reached a contradiction since the left-hand-side is a non-zero rational number with denominator dividing  $pq^2$ , which must be at least  $1/pq^2$  in size. It follows that our **assumption** must have been false, which implies that there exists a quadratic non-residue  $n$  satisfying  $|n| < p^\epsilon$ .

## References

- [1] A. Brauer, On the Non-existence of the Euclidean Algorithm in Certain Quadratic Number Fields, *Amer. J. of Math.* **62** (1940), 697-716.
- [2] D. A. Burgess, A Note on the Distribution of Residues and Non-residues, *J. London Math. Soc.* **38** (1963), 253-256.
- [3] R. Hudson, On a Conjecture of Issai Schur, **J. Reine Angew. Math.** **289** (1977), 215-220.
- [4] P. Hummel, On Consecutive Quadratic Non-residues: A Conjecture of Issai Schur, *J. Number Theory* **103** (2003), 257-266.